PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-195278
(43)Date of publication of application : 15.07.1992

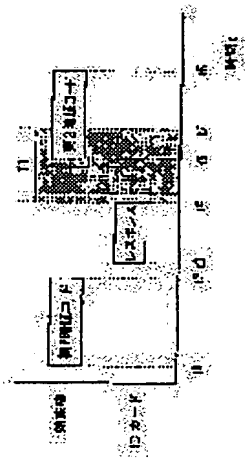
(51)Int.CI. G06K 17/00
G06F 15/30
G06F 15/30
G07F 7/12

(21)Application number : 02-320338
(22)Date of filing : 22.11.1990

(71)Applicant : DAINIPPON PRINTING CO LTD
(72)Inventor : YOSHIDA HIDEYO

(54) SECURITY CHECKING DEVICE

(57)Abstract:
PURPOSE: To effectively perform security check even when a password code and a procedure are recognized by others by inputting the next password code within a prescribed time after inputting one password code, and performing the check.
CONSTITUTION: A user inputs a first password code to a terminal after inserting an IC card to the terminal. Thereby, it is checked whether or not the first password code is correct, and a response can be obtained from an IC card side based on the result of check. The user recognizes the response by a display provided at the terminal, and inputs a second password code. Thereby, it is checked whether or not the second password code is correct, and access can be permitted only when both password codes are correct. At this time, a security condition that the second password code should be inserted within the prescribed time after inserting the first password code is set. In such a way, it is possible to effectively perform the security check even when the password code and an authentication procedure are recognized by a third party.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−195278

⑤1Int.Cl.[5]	識別記号	庁内整理番号	⑬公開　平成4年(1992)7月15日
G 06 K 17/00	T	6711−5L	
G 06 F 15/30	340	6798−5L	
	350	6798−5L	
G 07 F 7/12		8111−3E	G 07 F 7/08　B

審査請求　未請求　請求項の数 1　(全4頁)

⑤4発明の名称　セキュリテイチエツク装置

⑳特　願　平2−320338
㉒出　願　平2(1990)11月22日

⑦2発明者　吉田　英世　東京都新宿区榎町7番地　大日本印刷株式会社内
⑦1出願人　大日本印刷株式会社　東京都新宿区市谷加賀町1丁目1番1号
⑦4代理人　弁理士　志村　浩

明　細　書

1．発明の名称

セキュリティチェック装置

2．特許請求の範囲

複数の暗証コードを入力することにより、セキュリティをチェックする装置において、第1の暗証コードが入力された後、所定の時間帯内に第2の暗証コードが入力されることをチェックのための一条件としたことを特徴とするセキュリティチェック装置。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明はセキュリティチェック装置、特に複数の暗証コードの入力によりセキュリティチェックを行う装置に関する。

〔従来の技術〕

電子機器を用いた情報処理が普及するにつれて、高度なセキュリティを必要とする電子機器も増えている。たとえば、プリペイドカードや、今後普及が予想されるICカードなどが不正に使用された場合、大きな社会問題となる。このため、電子機器を用いた種々の情報処理システムでは、システムへのアクセスを許可する前にセキュリティチェックを行うのが一般的である。通常は、正当な使用者のみが知る暗証コードを入力させ、この暗証コードが正しいか否かをチェックする方法が採られる。また、セキュリティをより向上させるために、複数の暗証コードを所定の順序で入力したり、より複雑なアルゴリズムに基づく認証手順を行ったり、暗証コードやその入力手順を所定の回数以上間違えた場合には二度とそのシステムへのアクセスができなくなるようなロックを行ったりする方法も採られている。

〔発明が解決しようとする課題〕

上述のように、セキュリティをより向上させるために、種々の手段が講じられているが、従来の方法ではいずれも、正しい暗証コードや正しい認

証手順を第三者に知られてしまうと、この第三者に対してセキュリティは意味をなさなくなる。特に、今後普及が期待されているＩＣカードでは、個人のプライバシーに関わるデータが記録されることになり、第三者に不正にアクセスされる事態が生じると重大な問題となる。

そこで本発明は、暗証コードや認証手順を第三者に知られた場合でも、有効に機能することのできるセキュリティチェック装置を提供することを目的とする。

〔課題を解決するための手段〕

本発明は、複数の暗証コードを入力することによりセキュリティをチェックする装置において、第１の暗証コードが入力された後、所定の時間帯内に第２の暗証コードが入力されることをチェックのための一条件としたものである。

〔作　用〕

本発明によるセキュリティチェック装置では、暗証コードを入力する時点の時間的要素がチェックのための条件に付加される。すなわち、複数の暗証コードを入力させ、これらが正しいものか否かをチェックする従来の装置において、更に、第１の暗証コードが入力された後、所定の時間帯内に第２の暗証コードが入力されることを条件として付加している。正当な使用者には、暗証コードや認証手順の他に、この所定の時間帯が知らされることになる。したがって、万一、第三者が暗証コードや認証手順を知った場合であっても、第２の暗証コードを偶然にこの時間帯内に入力しない限り、セキュリティは確保される。

〔実施例〕

以下、本発明を図示する実施例に基づいて説明する。ここでは、本発明をＩＣカードに適用した例を述べる。ＩＣカードは、通常、各個人個人に対して発行されるカードであり、現在普及している磁気カードに比べ、演算処理機能を有し記憶容量も大きいという点に特徴をもち、今後は広く普及することが期待されている。このＩＣカードをアクセスして、内部のデータを読み出したり、内部にデータを書き込んだりする操作は、正当な使用者以外はできないようにしなければならない。ＩＣカードに対するアクセスは、一般には端末機によって行われる。この端末機には、データ読取／書込装置が内蔵されており、使用者はこの端末機にＩＣカードを挿入した上で、所定の操作をすることによりＩＣカードへのアクセスを行うことになる。このようなＩＣカードへのアクセスを許可する前に、所定のセキュリティチェックを行う必要がある。

第１図は本発明の一実施例に係るセキュリティチェック装置におけるセキュリティチェック方法の概念を示すタイムチャートである。チャートの上段は端末機への入力操作のタイミングを示し、下段はＩＣカードからのレスポンスのタイミングを示す。使用者は、ＩＣカードを端末機に挿入した後、第１暗証コードを端末機に入力する。すると、この第１暗証コードに対して正しいか否かがチェックされ、その結果に基づき、ＩＣカード側からレスポンスが得られる。使用者はこのレスポンスを端末機に備わっているディスプレイ装置などの画面で認識することができる。続いて、使用者は、端末機に対して第２暗証コードを入力する。すると、この第２暗証コードに対しても正しいか否かがチェックされる。こうして、２つの暗証コードがともに正しい場合にのみ、このＩＣカードへのアクセスが許可される。

以上は、従来装置でも行われた方法であるが、本発明の特徴は、第２暗証コードの入力時間に制限を設けた点にある。いま、横軸の時間軸に沿って、時刻ｔ１において第１暗証コードの入力作業を開始し、時刻ｔ２においてこの作業を終了したとする。そして、これに対して、時刻ｔ３～ｔ４の間にＩＣカード側からのレスポンスがあり、これに引き続いて、時刻ｔ５において第２暗証コードの入力作業を開始し、時刻ｔ６においてこの作業を終了したとする。この実施例では、「ＩＣカード側からのレスポンスが完了した時刻ｔ４から、所定の時間Ｔ１が経過する時刻ｔ７までに、第２暗証コードが入力されること」という付加的なチェック条件を設けている。すなわち、第２暗証コ

ードの入力開始時刻ｔ５は、図にハッチングを施して示した時間帯内（時刻ｔ４～ｔ７）になければならない。第２暗証コードの入力作業開始が、時刻ｔ７以後に行われた場合は、たとえ２つの暗証コードが正しいものであっても、セキュリティチェックの結果は不適合と判断され、ＩＣカードへのアクセスは許可されない。したがって、この時間帯の幅Ｔ１を、正当な使用者だけに知らせておくことにより、セキュリティの向上を図ることができる。

第２図は本発明の別な一実施例に係るセキュリティチェック装置におけるセキュリティチェック方法の概念を示すタイムチャートである。ここでも、チャートの上段は端末機への入力操作のタイミングを示し、下段はＩＣカードからのレスポンスのタイミングを示す。この実施例では、前述の実施例よりも更にセキュリティの向上が図れる。すなわち、この実施例では、「ＩＣカード側からのレスポンスが完了した時刻ｔ４より所定の時間Ｔ２が経過した時刻ｔ８から始まり、時間Ｔ３が経過する時刻ｔ９で終わるような時間帯（図にハッチングで示す部分）に、第２暗証コードが入力されること」という付加的なチェック条件を設けている。すなわち、第２暗証コードの入力開始時刻ｔ５は、図にハッチングを施して示した時間帯内（時刻ｔ８～ｔ９）になければならない。第２暗証コードの入力作業開始が、時刻ｔ８より前に行われても、時刻ｔ９より後に行われても、セキュリティチェックの結果は不適合と判断され、ＩＣカードへのアクセスは許可されない。別言すれば、第２暗証コードの入力作業開始が、早すぎても、遅すぎても、不適合となる。したがって、この時間帯の幅Ｔ２およびＴ３を、正当な使用者だけに知らせておくことにより、セキュリティの向上を図ることができる。たとえ第三者が、第１暗証コードおよび第２暗証コードを知り得たとしても、この第２暗証コードを入力するタイミングを知らない限り、このＩＣカードをアクセスすることは困難である。

時間帯の幅Ｔ１，Ｔ２，Ｔ３は、各ＩＣカードごとに独特な固定値としておいてもよいが、各アクセスごとに変動するようにしておくこともできる。この場合は、この認証作業を行う前に、何らかの時間設定コマンドで、各時間幅を変えることができるようにしておけばよい。なお、使用者が手作業で端末機に対する暗証コード入力を行う場合、上述の時間帯の幅があまり狭いと、正当な使用者であっても、所定の時間帯内に第２暗証コードの入力作業を開始することに失敗する場合もある。このような場合は、予め試行回数を所定値に設定しておき、失敗した場合でも何度か試行を繰り返すことができるようにしておくとよい。そして、この繰り返し行われた試行回数が所定値を越えた場合には、不正な使用が行われていると判断し、以後のアクセスを一切禁止するようなロック処理を行うとよい。また、暗証コードの入力を電子機器により自動的に行うようなシステムでは、上述の時間幅を非常に狭く（たとえば数ｍｓｅｃの単位）設定することができるので、セキュリティをより向上させることができる。なお、上述の実施例では、２つの暗証コードを続けて入力するシステムを例にとって説明したが、本発明は３つ以上の暗証コードを入力するシステムにも勿論適用可能である。また、セキュリティチェック処理は、端末機内部のプロセッサで行ってもよいし、ＩＣカード内部のプロセッサで行ってもよい。更に、上述の実施例では、ＩＣカードに対するアクセスシステムに本発明を適用したが、本発明は、セキュリティチェックを必要とするあらゆるシステムに適用可能である。

〔発明の効果〕

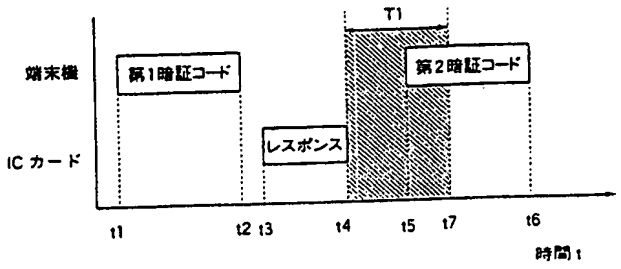
以上のとおり本発明によれば、複数の暗証コードを入力することによりセキュリティをチェックする装置において、第１の暗証コードが入力された後、所定の時間帯内に第２の暗証コードが入力されることをチェックのための一条件とするようにしたため、暗証コードや認証手順を第三者に知られた場合でも、セキュリティチェックを有効に機能させることが可能になる。

4．図面の簡単な説明

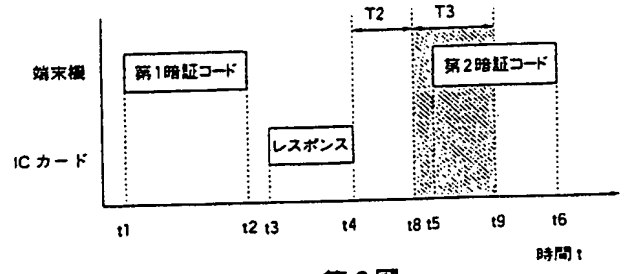
第1図は本発明の一実施例に係るセキュリティチェック装置におけるセキュリティチェック方法の概念を示すタイムチャート、第2図は本発明の別な一実施例に係るセキュリティチェック装置におけるセキュリティチェック方法の概念を示すタイムチャートである。

t1～t9…時刻、T1～T3…時間幅。

特許出願人　大日本印刷株式会社
出願人代理人　弁理士　志村　浩



第1図



第2図